**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

1-13 (Cancelled)

14. (Currently Amended) A method for verifying a signature, or respectively an authentication, utilizing an asymmetric private-key (d) and public-key (e, n) cryptographic calculation process between a "*prover*" entity comprising a terminal having first computing means provided with a first computing capacity and a "*verifier*" entity comprising second computing means provided with second computing capacity lower than said first computing capacity, said prover entity including electronic communication means for communicating with said verifier entity, wherein the prover entity performs first cryptographic calculations with said private key (d) to produce a signature calculation, or respectively an authentication value, constituting response data, and the verifier entity, based on said response data, performs second cryptographic calculations with said public key to perform said signature verification, or respectively said authentication, the first and second cryptographic calculations serving to implement the calculation of modulo-n or large-number multiplications, wherein the cryptographic calculation process uses said public key comprising a public exponent e and a public modulo n, and said private key comprising a private exponent, said method further comprising:

using said first computing means for calculating at the level of said prover entity

at least one prevalidation value;

using electronic communication means of the prover entity for transmitting to the

verifier entity said response data comprising at least said prevalidation value,; and

utilizingretrieving said prevalidation value by the verifier entity and using said

second computing means forto perform performing at least one modular reduction by

utilizing said prevalidation value to obtain the remainder of the modulo calculation,

without any division operation at the level of the verifier entity.


15. (Previously Presented) A method according to claim 14, wherein for a public

exponent e=2, and wherein the cryptographic calculation process is based on a RABIN

algorithm, said prevalidation value comprises a unique value, which is the quotient Q of

the square of said respective value of a signature or a response by said public modulo n, Q

= R*R/n, where R designates said respective value of a signature or a response to an

authentication.


16. (Previously Presented) A method according to claim 15, wherein after the

reception by said entity of said respective value of a response to an authentication

verification or a signature of a message (M), and of said at least one prevalidation value

comprising said quotient, said method comprises, at the level of said verifier entity, the

following steps:

calculating the difference ($D_{AR}$, $D_{SR}$) between the square of the response value

R*R and the product Q*n of said quotient Q by said public modulo n, ($D_{AR}$, $D_{SR}$ = R*R

=Q*n; and

verifying the equality of said difference with the value of a function of said

response value, without any division operation by the modulo n operation.

17.    (Previously Presented) A method according to claim 14, wherein for a

public exponent $e = 3$, and wherein the cryptographic calculation process is based on an

RSA algorithm, said at least one prevalidation value comprises:

a first quotient $Q_1$ of the square R*R of said response value R by said public

modulo n; and

a second quotient $Q_2$ of the product of said response value and the difference

between the square R*R of said response value and the product of said first quotient $Q_1$

and the public modulo n, by said public modulo n, $Q_2 = R*(R*R - Q_1*n)/n$.

18.  (Previously Presented) A method according to claim 17, wherein after the

reception of said response value R and said at least one prevalidation value comprising

said first and second quotients $Q_1$ and $Q_2$, said method comprises, at the level of said

verifier entity, the following steps:

calculating the difference ($D_{ARSA}$, $D_{SRSA}$) between the product of said response

value R and the difference between the square R*R of this response value and the product

of said first quotient $Q_1$ and the public modulo n, and the product of said second quotient

$Q_2$ and said public modulo n ($D_{ARSA}$, $D_{SRSA}$) = $R*(R*R - Q_1*n)-Q_2*n$; and

verifying the equality of this difference with the value of a function of said

response value, without any division operation by modulo n operation.

19. (Previously Presented) A method according to claim 16, wherein for an operation for verifying a signature of a message (M), said function comprising a standardized public function f(M) of said message M, said method comprises the following steps:

applying a condensation function to said message to obtain a message digest CM; and

concatenating said message digest with a constant value.

20. (Previously Presented) A method according to claim 18, wherein for an operation for verifying a signature of a message (M), said function comprising a standardized public function f(M) of said message M, said method comprises the following steps:

applying a condensation function to said message to obtain a message digest CM; and

concatenating said message digest with a constant value.

21. (Previously Presented) A method according to claim 16, wherein for an authentication verification operation, said method further comprises the step of transmitting a prompt value from the verifier entity to the prover entity.

22. (Previously Presented) A method according to claim 18, wherein for an authentication verification operation, said method further comprises the step of transmitting a prompt value from the verifier entity to the prover entity.

23. (Previously Presented) A method according to claim 21, wherein said prompt value comprises a random value A modulo n, said response value R comprises an encrypted value B, and said function of the response value comprises a function f(A) of said random value A.

24. (Previously Presented) A method according to claim 22, wherein said prompt value comprises a random value A modulo n, said response value R comprises an encrypted value B, and said function of the response value comprises a function f(A) of said random value A.

25. (Previously Presented) A method according to claim 16, wherein said function f(A) of said random value A comprises a function among the functions f(A) = A, f(A) = n-A, f(A) = C*A modulo n, f(A) = -C*A modulo n.

26. (Previously Presented) A method according to claim 21, wherein said function f(A) of said random value A comprises a function among the functions f(A) = A, f(A) = n-A, f(A) = C*A modulo n, f(A) = -C*A modulo n.

27. (Previously Presented) A method according to claim 22, wherein said function f(A) of said random value A comprises a function among the functions f(A) = A, f(A) = n-A, f(A) = C*A modulo n, f(A) = -C*A modulo n.

28. (Previously Presented) A method according to claim 25, wherein at the level of the verifier entity, the calculation of said function f(A) = C*A modulo n comprises

calculation of the value C*A and storing of said value if C*A < n, and the calculation and storing of the value C*A-n if not, and in that calculation of said function f(A) = -C*A modulo n comprises calculation of the value n-C*A and storing of said value if n-C*A ≥ 0, and otherwise calculation of the intermediate value C*n-C*A, and if said intermediate value is greater than or equal to zero, calculation and storing of the value of -C*A modulo n, for verifying the equality of said authentication without any division for the modular reduction.

29. (Previously Presented) A method according to claim 26, wherein at the level of the verifier entity, the calculation of said function f(A) = C*A modulo n comprises calculation of the value C*A and storing of said value if C*A < n, and the calculation and storing of the value C*A-n if not, and in that calculation of said function f(A) = -C*A modulo n comprises calculation of the value n-C*A and storing of said value if n-C*A ≥ 0, and otherwise calculation of the intermediate value C*n-C*A, and if said intermediate value is greater than or equal to zero, calculation and storing of the value of -C*A modulo n, for verifying the equality of said authentication without any division for the modular reduction.

30. (Previously Presented) A method according to claim 27, wherein at the level of the verifier entity, the calculation of said function f(A) = C*A modulo n comprises calculation of the value C*A and storing of said value if C*A < n, and the calculation and storing of the value C*A-n if not, and in that calculation of said function f(A) = -C*A modulo n comprises calculation of the value n-C*A and storing of said value if n-C*Á ≥ 0, and otherwise calculation of the intermediate value C*n-C*A, and if said intermediate

value is greater than or equal to zero, calculation and storing of the value of -C*A modulo

n, for verifying the equality of said authentication without any division for the modular

reduction.

31. (Previously Presented)A method according to claim 23, wherein said function

f(A) of said random value A is the function f(A) = A, which makes it possible to verify

the equality of said difference and the validity of said authentication without any division

operation for the modular reduction.

32. (Previously Presented) A method according to claim 24, wherein said

function f(A) of said random value A is the function f(A) = A, which makes it possible to

verify the equality of said difference and the validity of said authentication without any

division operation for the modular reduction.

33. (Previously Presented) A method according to claim 14, wherein said

response value, an encrypted value B, and a quotient value Q are concatenated prior to

transmission of the values from the prover entity to the verifier entity.

34. (Previously Presented) A method according to claim 14, wherein the verifier

entity compression embedded system and the prover entity comprises an embedded card

reading system.